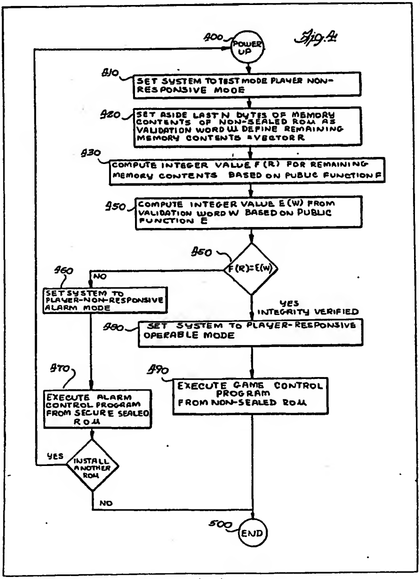
(12) UK Patent Application (19) GB (11) 2 121 569 A

(21) Application No 8312834
(22) Date of filing 10 May 1983
(30) Priority data
(31) 377413
(32) 12 May 1982
(33) United States of America (US)
(43) Application published 21 Dec 1983
(51) INT CL³ G06F 15/44
(52) Domestic classification G4A 13E 17B AP G4H 13D 14A 1A TG
(56) Documents cited EP A 0033833 EP A 0005179 US 4186871
(58) Field of search G4A G4H
(71) Applicants
Bally Manufacturing Corporation, (USA-Illinois), 2640 West Belmont Avenue, Chicago, State of Illinois 60618, United States of America.
(72) Inventors
Martin Anthony Keane
(74) Agent and/or Address for Service
Boult, Wade and Tennant, 27 Furnival Street, London, EC4A 1PQ.

# (54) System guaranteeing integrity of a gambling system

(57) Data and associated validation information stored in a nonsecure location are verified as to integrity by cryptograph techniques. Verification activates a gambling system to operate in a gambler-responsive mode, and non-verification activates an alarm mode. The system is used in postal metering, electronic mail, electronic funds transfer and other source data processing systems. The validation information is formed by deriving a first value from the data according to a first relationship, and then deriving the validation information from the first value by means of a nonpublic derivation having an inverse function. The validation word is then associated with the data and stored in the nonsecure portion. Verification is accomplished by deriving 430 a first value from the data

(57) continued overleaf...




GB 2 121 569 A

This specification as filed includes a computer program which is not here reproduced.

by the first relationship, and deriving 450 a second value from the validation information by means of the inverse function. The first and second values are operatively related 450 to determine system integrity. All relationships are one way functions, in a preferred embodiment. In a preferred embodiment, the first and inverse second relationships are public and the second relationship is secret.

2121569

Fig.1

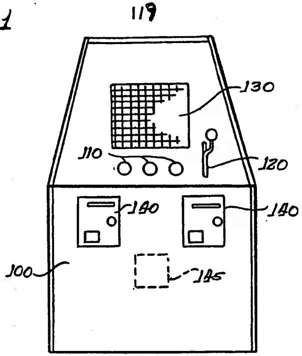
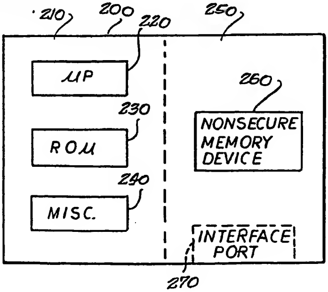



Fig.2.



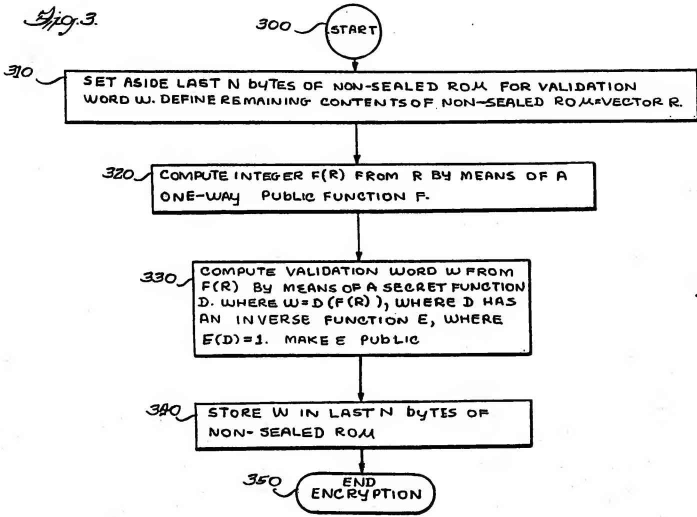

START
300
SET ASIDE LAST N bytes OF NON-SEALED ROM FOR VALIDATION WORD W. DEFINE REMAINING CONTENTS OF NON-SEALED ROM=VECTOR R.
310
COMPUTE INTEGER F(R) FROM R BY MEANS OF A ONE-WAY PUBLIC FUNCTION F.
320
COMPUTE VALIDATION WORD W FROM F(R) BY MEANS OF A SECRET FUNCTION D. WHERE W=D(F(R)), WHERE D HAS AN INVERSE FUNCTION E, WHERE E(D)=1. MAKE E PUBLIC
330
STORE W IN LAST N bytes OF NON-SEALED ROM
340
END ENCRYPTION
350

Fig.3.

2121569

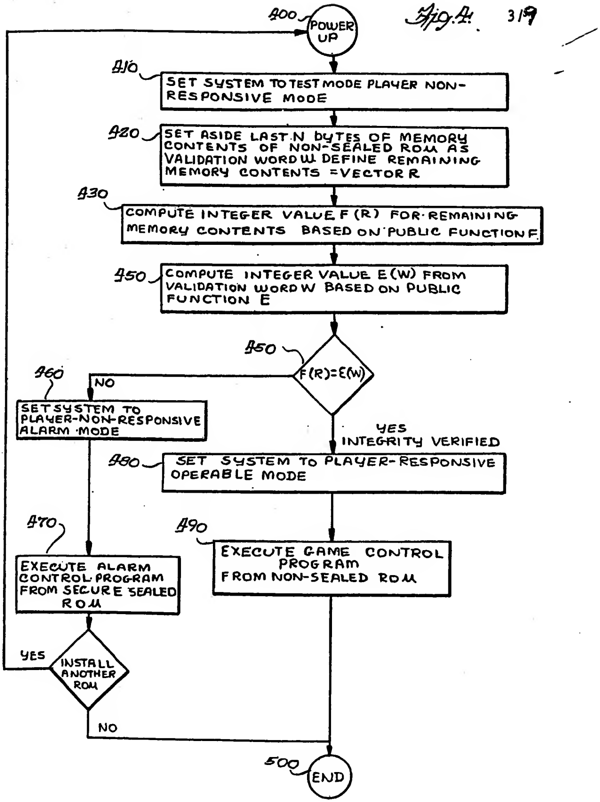


Fig.4 3/9
400
POWER UP
410
SET SYSTEM TO TEST MODE PLAYER NON-RESPONSIVE MODE
420
SET ASIDE LAST N bytes OF MEMORY CONTENTS OF NON-SEALED ROM AS VALIDATION WORD W. DEFINE REMAINING MEMORY CONTENTS =VECTOR R
430
COMPUTE INTEGER VALUE F (R) FOR REMAINING MEMORY CONTENTS BASED ON PUBLIC FUNCTION F
450
COMPUTE INTEGER VALUE E(W) FROM VALIDATION WORD W BASED ON PUBLIC FUNCTION E
450
F(R)=E(W)
460
NO
SET SYSTEM TO PLAYER-NON-RESPONSIVE ALARM MODE
YES
INTEGRITY VERIFIED
480
SET SYSTEM TO PLAYER-RESPONSIVE OPERABLE MODE
470
490
EXECUTE ALARM CONTROL PROGRAM FROM SECURE SEALED ROM
EXECUTE GAME CONTROL PROGRAM FROM NON-SEALED ROM
YES
INSTALL ANOTHER ROM
NO
500
END

SPECIFICATION

## A system and method for guaranteeing the integrity of a gembling system

This invention relates to secure systems, such as gambling apparatus, and more particularly to a system for guaranteeing the integrity of information content in the secure system, such as the control program of gambling apparatus.

It is often the case in electronic gambling systems that a microprocessor electronics based gambling system can be customized for different types of play by changing a memory device (such as an EPROM) or by changing the memory device contents (such as by remotely downloading date into a read-write memory (RAM or EPROM). However, it is currently the practice of some stete gambling commissions, such as New Jersey, U.S.A. to require a seel be applied to all circuitry on each circuit boerd (including the EPROM or RAM) as part of the certification process. Thus, inventories must be maintained of the sealed boards for each of a plurality of machines, both in manufacturing output end maintaining a repair stock pile. This epproach is both costly and inefficient, inasmuch as meny machines have a common nucleus and utilize the same circuit board with a different control memory program for each of a plurality of games being selected by interchanging a memory device or its contents.

Although this approach is costly and cumbersome, there has heretofore been no alternative technique provided to perform the important function of guaranteeing the integrity of the gambling machines.

In accordance with one aspect of the present invention, a system is provided wherein data end associated validation information stored in e nonsecure location are verified as to integrity by cryptographic techniques. Good integrity verification activates the system to operete in a first mode, and bad integrity verification activates the system to operate in a second mode. In a preferred embodiment, the system is a gambling system, with a first mode corresponding to user responsive operation and the second mode corresponding to an alarm mode. Other systems where the present invention would be useful include postal metering, electronic mail, electronic funds transfer and other secure data processing systems.

In accordance with another aspect of the present invention, the system has an interface port for communicating with an external device, such as a central control computer. Data and associated validation information are loaded into memory in the nonsecure location, and the system verifies the integrity of the data and associated validation information as stored in the memory by cryptographic techniques operatively relating the data to the associated validation word. The system is activated to either a first or second operative mode responsive to a verification result of good or bad integrity, respectively.

For example, a central computer could download information to one or a plurality of remotely located systems which would each verify the integrity of the information received and stored in its respective memory. Where the remotely located systems ere gembling systems, the downloaded information can be odds, control programs, random number seeds, etc.

In accordance with one of the illustrated embodiments of the present invention, a gambling apparatus is disclosed having a secure portion which is certified and sealed by the Gaming Commission, and having a nonsecure portion, not sealed by the Gaming Commission, the integrity of which is verified by the secure portion. The secure portion of the gambling apparatus comprises a circuit board having a central processor and a first memory. The nonsecure portion of the gambling apparatus is comprised of a second portion of the circuit board, or an independent circuit board, having a second memory such as a nonsecure ROM, EPROM, or read-write memory (RAM). Utilizing cryptographic techniques, the integrity of the nonsecure portion of the system is verified by the secure portion of the system.

The gambling system is opereble in three modes, and powers up in a test mode for verifying the integrity of the gambling system. Where a positive verification is made that the nonsecure memory (e.g. ROM) has satisfactory integrity, the system is activated to an operable mode responsive to player user control inputs. Alternatively, where the results of the test mode is e negative verification showing the nonsecure memory does not have good integrity, and gambling system is forced to an inoperable mode nonresponsive to player user control inputs, and an alarm is activated.

The nonsecure portion of the circuit board, the integrity of which is cryptographically detectable, has a first nonvolatile memory (such as a ROM, PROM, EPROM or EEPROM nonvolatile memory or a read-write (RAM) volatile memory) having a validation word stored therein, the validation word being derived from the first memory contents according to a first relationship. The validation word is formed by deriving a first value from the first memory's contents. The validation word is then derived from the first value by means of a nonpublic derivation having an inverse function. The validation word is then combined to form a part of the contents of the first memory.

The secure portion of the circuit board has a processor and a second nonvolatile memory mounted thereon. The integrity of the secure portion is overt and detectable, such as by physical seal. The secure portion of the board includes means for deriving a second value from the validation word of the first memory means of the inverse function. The secure portion also includes means for comparing the first and second values, and means for verifying the integrity of the second memory. The verification means activates the gaming system to the user reponsive play mode responsive to a comparison result of equality, or activates the gaming system to the user nonresponsive (alarm) mode responsive to a comparison result of inequality. The relationship for deriving the first value, the nonpublic relationship, and the inverse relationship of the

non-public relationship, are such that interrelating or cross deriving one to another is very complex and an extremely difficult and time consuming task. In a preferred embodiment, tha encryption function is secret and the inverse function is public.

A better understanding of the invention may ba had from tha following detailed examples, the detailed description being taken in conjunction with tha accompanying drawings in which:

*Figure 1* is a perspective view of a gaming system such as a video slot gambling machine, illustrating one apparatus which can utilize the present invention;

*Figure 2* is a top view showing one embodiment of a circuit board as contained in the gaming system of Figure 1 having a secure portion and a nonsecure portion;

*Figure 3* is a flow chart illustrating one embodiment of the encryption method utilized in accordanca with one embodiment of the present invantion;

*Figure 4* is a flow chart of the decryption/test method as utilized in accordance with one embodiment of the present invention; and

*Figure 5A-D* are computer program listings for one embodiment of the present inention.

Referring now to Figure 1, a gaming system is shown illustrative of one embodiment of the present invention. A housing 100 is provided which contains the necessary human player control interfaces as well as electronic circuitry and mechanical circuitry. Human player control inputs ara provided, such as push buttons 110 and control handle 120. A viawing area, 130 such as video screen is provided on tha front of the cabinet housing 100 for player viewing of the gaming machine response to player inputs. Coin shoots 140 are provided for accepting player coins and returning bent coins. The number of credits which tha player has as well as the active game display are provided on the visual display means 130. For exampla, the gaming system of Figure 1 can be a slot machine gambling system having 3, 4, or any number of raels, or may alternatively be any other type of gaming or gambling system. Where applicable, a pay out shoot 145 may be provided for outputting coins to winning players.

The housing 100 also contains an electronic circuit board 200, as shown in Figure 2, which provides the control and game electronic circuitry necessary to create the desired gambling system in conjunction with the video display 130 and user interface controls 110 and 120. Additionally, the housing 100 contains necessary power supplies, limit switches, etc. necessary to implement the remainder of the desired gaming system.

Referring to Figure 2, the circuit board 200 as discussed with reference to Figure 1 is shown in block diagram form. The circuit board 200 may be comprised of a single circuit board or of a plurality of circuit boards with appropriate interconnections provided. The circuit board 200 is comprised of two functionally separate units, a sealed secured portion 210 and a nonsealed, nonsecure circuit portion 250. The sealed circuit board portion 210, as illustrated, contains a microprocessor 220, a read only memory (such as a ROM, PROM, or EPROM), and miscellaneous electronic and electromechanical circuitry 240. The sealed portion of the circuit board 210 represents the sealed portion of the gaming system in a physical sealing manner which would comply with a particular State Gaming Commission's requirements.

The nonsealed portion of the circuit board, 250, contains an interconnection sockat 260 for a memory device, (e.g. for a RAM, ROM, PROM, or EPROM). When the socket 260 provides interconnection for a read-write memory, RAM or EPROM, the data contents of the read-write memory can be downloaded into the read-write memory. For example, a control program can be down-loaded from a remota site into the read-write memory of a local gambling system via an interface port 270 (Figure 2) of tha local gambling system and the downloaded program verified by the secura portion of the circuit board in accordance with the teachings of tha present invention. Multiple gambling systems can be configured to meet crowd selection pattems by specifying control programs either locally or remotely for each system. Tha systems can also be selectively forced inoparative by downloading appropriate control programs. This portion of tha circuit board is not physically sealed, and thus the memory inserted into the ROM socket 260 can aasily be changed or interchanged. Whila this is desirable from the view point of minimizing spara parts stock piling and maximizing manufacturing flexibility, the nonsealed socket does pose security risks and problems. However, in accordance with the present invention, cryptographic techniques are utilized to verify the integrity of the nonsecure portion of tha circuit board, 250, via means of cryptographic processing by the secure portion of the circuit board, 210. The microprocessor 220 may be of any type, with its selection being made based upon desired operating speed, instruction set capabilities, and cost considerations. In addition, the microprocessor 220 may be comprised of a plurality of circuits including a general purpose microprocessor (of a 4, 8, 16, 32, etc. bits register length), in conjunction with special purpose peripheral processors and interfaca chips, such as numbar crunchers, fast Fourier processors, fast multipliers, etc.

Referring to Figures 3 and 4, the methodology utilized to accomplish the invention of the illustrated embodiments can be more readily understood by reference to the encryption (Figure 3) and decryption (Figure 4) flow charts.

Referring to Figure 3, the encryption process utilized for creating a verifiably secure memory for insertion into the nonsealed socket 260 (of Figure 2) is illustrated in flow chart form. The procedure starts at step 300. Proceeding at step 310 the last N bytes of the nonsecura memory are designated as a validation word W and reserved from the remaining contents of tha nonsecure memory which is designed as the vector R. A control program which has been developed is loaded into the encryption systems memory and designated as the contents of the nonsealed and nonsecure memory (the vector R). The validation word W is as yet undefined,

but will represent the encrypted key to insure the integrity of tha remainder of the contents of tha memory.

Proceeding to step 320 en integer value F(R) is computed from the vector R by meens of e one way public function F. F is a one way function mapping R into en integer whose magnitude is comparable to thet of one element of R. F need not be one to ona, but should be such that changing R while leaving F(R) unchanged is a difficult task. The function F is a public function in that it is also utilized in the encryption process end may be discovared or known by members of the public.

Proceeding to step 330, e validation word W is computed from the value F(R) by means of a secret function D which meps words into words with an inverse function E which is e public encryption function. Thus, W = D(F(R)), and E(D) = 1. Thus, when the function E is utilized in the encryption process, E (W) should equal F(R) only when the contents of tha memory (the vector R and the velidetion word W) has not been tampered with. Thus, the integrity of tha contents of the nonsealed nonsecure memory can be verified.

Proceeding to step 340, the validetion word W is placed in the memory locations which had been set eside as tha last N bytes of the nonsealed memory. At this point the encryption proces has ended as evidenced at step 350. The contents of the nonseeled memory (vector R) plus the validation word (eppropriately located in the last N bytes) can be committed to the nonsecure end nonseeled memory (e.g. ROM, EPROM, RAM).

For further details on one way mapping functions, and public key cyrptography concepts, reference is made to the litereture in general, such as "A Method for Obtaining Digital Signatures end Public Key Cryptocism Systems", by R.L. Rivest, et el., as published in the February, 1978, Volume 21, Number 2 issue of the *Communications of the ACM*, at pages 120-126, hereby incorporeted herein by raference. A second reference, "The Methemetics of Public Key Cryptography" by Martin E. Hellman, published in Scientific American, pages 146-157, 19, deals generally with tha mathematics involved in public key cryptogrephy, and is hereby incorporated herein by reference. Both of the aforementioned references deel with the general problem of secure electronics communication system, either for message transfer, or for funds transfer. The references address themselves to techniques to prevent tampering with new electronic communication systems end fund transfer systems and meens to protect the vest quantities of private information such as credit records end medical history stored in computer data banks. Encryption end decryp- tion are utilized for transforming information so that it is unintelligible end therefore useless to those who are not meant to have access to it. Secondly, cryptographic techniques are utilized to insure that messages sent have not been tampered with, of critical concern in electronic funds transfer.

Referring to Figure 4, the decryption process is illustrated in flow chart form, illustreting one embodiment of the present invention. The process flow sterts when tha gambling system of Figura 1 is powered up, at step 400. The process proceeds to step 410 where the system is set to the test mode, wherein the system is nonresponsive to players control inputs. The contents of the nonsealed portion of the circuit board are examined by the secura seeled portion of the circuit board, by defining the last N bytes of the nonsealed memory contents as the velidetion word W, end defining the remaining nonseeled memory contents as a vector R, whose elements ere the individuel words of the nonseeled memory.

Proceeding, as illustrated at step 430, the integer value F(R) is computed for the nonsealed memory contents represented es the vactor R by means of the public function F. Next, en integer velue E(W) is computed from the validation word W based upon tha public encryption function E. It will be recalled that the function E is the inverse of the function D. Thus, E(W) = E(D(F(R))) = F(R) only when the contents of the nonsealad memory heve not been tampered with.

The decryption process proceeds as illustrated at stap 450, where the computed velue F(R) is compered to the computed velue E(W). If F(R) = E(W), then the integrity of the nonsealed memory has been positively verified, and the geming system flow proceeds as illustrated at step 480. The gaming system is set to a player responsive operable mode, wherein the coin chute and user controls ere ectiveted end the gaming system becomes playabla, as illustrated at step 490. The control program contained in the nonsealed memory is executed by the processor in the sealed portion of the circuit boerd, 210, and the gaming system operation proceeds under supervision of the control progrem. At this point, the decryption end integrity verification procedure has been completed, as illustrated at step 500.

Referring back to decision block 450, where the result of the comparison of F(R) and E(W) results in e determinetion of inequality, the procedureal flow continues as illustrated et step 460. The gaming system of Figure 1 is set to e pleyer nonresponsive alarm mode. The user controls become inoperetive, end the system proceeds to execute an alerm control program, as preferably stored in the secure sealed ROM illustrated at step 470. At this point the machine is disabled, and the operator is informed of the error condition. The tainted nonsealed memory device is removed from the nonsealed socket and the operator can choose between shutting the system down, or trying en alternte non-sealed memory integrated circuit. Whera the system is shut down, the procedural flow is ended, as illustrated at block 500. Where a new integrated circuit is placed in the ROM sockat 460, the decryption procedure repeats starting again at step 400 with power up. In either event, the tainted memory chip should be turned over to authorities for evaluation as to tampering or simply system or manufacturing error.

Thus, in accordance with the discussion of the illustrated embodiment, herein, the ROM 230 in the sealed portion of tha circuit board, 210, contains a verification program to monitor the security of the nonsealed portion of the circuit board 250 containing tha pluggad in nonsealed mamory 260. The function F is a plublicly availabla function such that the signature F(R) provides a publicly available signature of the nonsealed memory contents less the validation check word W, while the encryption function E is publicly

available to provide for a publicly available encryption key check word E(W). By computing the validation check word W using a secret decryption key, function D, which is the inverse of the public encryption function E, the integrity of the entire contents of the nonsealed memory (both the validation word W and the remaining contents) can be protected and detected in accordance with the present invention's teachings.

An example may be illustrative. Presume the nonsealed memory to be protected is an EPROM having a capacity of 2048 bytes. The last 8 bytes are set aside as the validation word W, and the remainder is partitioned into 408 five byte words ($D_0$, $D_1$ ... $D_{407}$). Define 408 prespecified integers ($P_1$, $P_2$, ... $P_{407}$) and an additional prespecified integer $P_{408}$. Additionally, a large composite integer XNBase is prespecified. F(R) and E(W) can then be computed as follows:

$$F(R) = \sum_{i=0}^{i=407} W_i^{P_i} (\text{modulo XNBase}).$$

$$E(W) = W^{P_{408}} (\text{modulo XNBase}).$$

The validation check procedure can be modified slightly such that if F(R) plus E(W) (modulo XNBase) equal to 0 then the integrity of the EPROM is questioned and the system goes to the alarm mode. This example in its modified format has been implemented with a BASIC language program and has been successfully tested on an EPROM from an electronic slot machine. The BASIC language program and EPROM object code hexdump listing are illustrated in Figures 5a-d. While BASIC language was utilized in the illustrated program of Figure 5, any computer programming language could be utilized with an appropriate system. In the illustrated system of Figures 1-5, all arithmetic operations were exact modulo (XNBase), double precision numbers exact to 16 digits. However, other cryptographic mathematical techniques could be utilized equally well, and implemented in accordance with the teachings of the present invention.

It will be understood by those skilled in the art that other functional and operative relationships between the data and validation information can be used consistent with the teachings of the present invention. Furthermore, in performing the verification function, operative relationships in addition to or instead of comparison can be used consistent with the teachings of the present invention.

While there have been described above various embodiments of system and methods for guaranteeing the integrity of the control program of a gambling machine having sealed and nonsealed portions, for the purpose of illustrating the manner in which the invention may be used to advantage, it will be appreciated that the invention is not limited thereto. Accordingly, any modification, variation, or equivalent arrangement within the scope of the accompanying claims should be considered to be within the scope of the invention.

## CLAIMS

1. A system for selectively operating in one of a plurality of modes responsive to a determined system integrity comprising:
   (a) a nonsecure portion of the system having data and validation information in a portion therein,
   (b) a secure portion of the system comprised of:
      (1) means for deriving a first value from the data according to a first relationship;
      (2) means for deriving a second value from said validation information by means of a second relationship,
      (3) means for operatively relating said first and second values to determine system integrity,
      (4) means for activating said system to a selected operational mode responsive to said means for operatively relating,
2. The system as in Claim 1 further characterized in that said nonsecure portion comprises a memory.
3. The system as in Claim 1 wherein the integrity of the nonsecure portion is cryptographically verifiable, and the integrity of the secure portion is noncryptographically verifiable.
4. The system as in Claim 1 further characterized in that said validation information is derived from said data according to first and third relationships.
5. The system as in Claim 4 wherein said second relationship is the inverse of the third relationship.
6. The system as in Claim 1 further characterized in that said means for operatively relating provides bad and good system integrity outputs indicative of the determined system integrity.
7. The system as in Claim 6 wherein said means for activating said system activates said system to a first operational mode responsive to good system integrity output and activates said system to a second operational mode to a bad system integrity output.
8. The system as in Claim 1 further characterized in that said system is activated to a first operational mode responsive to a determination of good system integrity and said system is activated to a second operational mode responsive to a determination of bad system integrity.
9. The system as in Claim 7 or 8 further characterized in that said first operational mode is a normal operational mode, and said second operational mode is an alarm mode.

10. The system as in Claim 4 or 5 wharain said first and second relationships are pubiic and said third relationship is secret.

11. Tha system as in Claim 4 or 5 wherein said first, second and third relationships are one way functions.

12. The system as in Claim 1 wherein said first relationship is further characterized in that changing any of the data changes tha first value.

13. Thay system as in Claim 1 furthar characterized as a gaming system.

14. The system as in Claims 1 or 2 or 3 or 4 or 5 or 6 or 7 or 8 or 12 further characterized as a gaming system.

15. The system as in Claim 10 further characterizad es a gaming system.

16. The system as in Claim 11 further characterized as a gaming system.

17. The systam as in Claim 9 further characterized as a gaming system.

18. Tha system as in Claim 17 whareln said noraml operation moda is a player-responsive mode.

19. The system as in Claim 13 further characterized in that said secura portion is physically saaled.

20. A system as in Claim 1 or 13 further characterized in that said data end validation information are loaded into said nonsecure portion from en apparatus remotely located relative to the system.

21. The system as in Claim 1 or 13 wherein said nonsecure portion includes a memory, and said secura portion includas a processor and a mamory.

22. The system as in Claim 1 or 13 further comprising:

interface means for communicating with a device external to tha system,

means for loading the nonsecure portion with received communications responsive to the interface means.

23. The system as in Claim 22 wherein said received communications is furthar characterized as said data and validation information.

24. The system as in Claim 22 further comprising:

means for communicating the determined system integrity to a devica external to the system.

25. The system as in Claim 1 or 13 wherein said secure portion of tha system is remotely located relative to said nonsecure portion.

26. Tha system as in Claim 1 or 13 wherein said secure portion comprises a processor and a memory, wharain seid processor executes instructions from said secure mamory to derive said first and second values.

27. The system as in Claim 8 furthar characterized in that said first mode is a player responsive mode, end said second mode is a player nonresponsive mode.

28. The mathod as in Claim 27 wherein said second mode activates an elarm.

29. A system for insuring tha integrity of a ramotely located downloadad memory comprising;

(a) a controller including encryption circuitry for deriving validation information from data by means of a first relationship and a second relationship having an inverse,

(b) a system, remotaly located relative to said controller, including e memory,

(c) maans for communicating data and validation information from said controller to said remotely located system for storage in said memory,

(d) varification maans comprised of:

(1) means for deriving a first value from the data contents of the memory by said first relationship;

(2) means for deriving a second value from said validation information by said inversa relationship;

(3) maans for operatively relating said first and second values for providing an output indicative of system integerity, and

(4) means for manifesting an action responsive to said system intagrity output.

30. Tha system as in Clalm 29 wherein said verification means is remotely located relative to said controller.

31. Tha system as in Claim 30 further characterized in that said first relationship and inverse sacond relationship are public and said second ralationship is secrat.

32. The system as in Claim 30 wherein said remotely located system is a gaming system.

33. The system as in Claim 30 wherein said first, second and invarse ralationships are one-way mapping functions.

34. The system as in claim 30 wherein said action is further characterized as activating said systam to a normal operable mode responsive to an output of good system integrity, and activating said system to an alarm mode responsiva to an output of bad system integrity.

35. The system as in Claim 30 wherein said remotely located system is further comprised of data processing means.

36. The system as in Claim 30 wherein said controllar is operatively coupled to selectively communicata with a plurality of remotely located systems.

37. Tha system as in Claim 36 further characterized in that at least one of said remotaly located systems is a gaming system.

38. The system as in Claim 37 wherein each of said remotely located systems is operatively configured responsive to communications from said controller to the respective remotely located system.

39. A gaming system comprising:

(a) a circuit board;

(b) a nonsecure portion of the circuit boerd, the integrity of which is cryptographically detectable, having e memory having data end validetion informetion stored therein, wherein the validetion information is derived from the data information according to e public first relationship end e secret second relationship heving e public inverse relationship;

(c) a secure portion of the circuit board having processing electronics mounted thereon, the integrity of the sacure portion being detectable,

wharein said secure portion of the circuit boerd is furthar comprised of:

(1) meens for deriving a first value from the data omfpr, atopm eccording to the public first relationship,

(2) maans for deriving a second value from said validation word by means of said public inverse relationship,

(3) means for operating on seid first and second values to provide an integrity signal,

(4) means for activeting said system to a first mode responsive to a first integrity signel indicative of good system integrity, and

(5) means for activating said systam to a second mode responsive to a second integrity signel indicative of bad system integrity.

40. The system as in Claim 39 wherein said secure portion is further comprised of a processor and a second memory.

41. The system as in Claim 39 wherein said first, second and inverse second relationships are one-way functions.

42. A system es in Claim 39:

wherein said first relationship hes the charactaristic thet changing the contants of seid memory chenges said first value.

43. Tha system of Cleim 39:

wherein said second relationship is a one-way trap-door function.

44. A gaming system comprising:

(e) a cabinet having e display eree and a user control;

(b) e circuit board mounted within the cabinet;

(c) a nonsecure portion of the circuit boerd, the integrity of which is cryptogrephicelly detectebie, having e memory heving deta and validation information stored therein, wherein the velidetion infomation is derived, by meens of a second reletionship heving an inverse relationship, from e first velue derived from and chenging eccording to e first relationship responsive to the data contents;

(d) a sacure portion of the circuit board heving verifiably good integrity comprising:

(1) maens for deriving e second value from the data contents of the first memory eccording to the first reletionship,

(2) means for deriving a third value from seid validation information by meens of said inverse ralationship,

(3) means for providing en integrity output responsive to operting on seid second end third velues,

(4) means for activating said system to a first mode responsive to e first integrity output, and

(5) means for activeting said system to a second mode responsive to e sacond integrity output.

45. The system as in Claim 44 wherein said first integrity output is indicative of good system integrity, and said second integrity output is indicative of bad system integrity.

46. Tha systam es in Claim 45 wherain said first mode is further characterized es ectivating said system to a usar control responsive system.

47. The systam as in Claim 45 or 46 wherein said second mode is further charactarized es activeting an alerm.

48. A gaming system operebie in a player responsive mode and an aiarm moda, comprising:

a first memory having data and validation information contents tharein, wharein said validation information is operatively associated with the remaining contents of the nonsecure memory

e secure memory;

means for velidating the integrity of the first mamory comprising:

meens for executing instructions from the secure memory so as to derive e first value operativaly associatad with the data contents of the first memory;

means for executing instructions from tha secure memory so as to derive a second value operatively associated with the validation information;

maens for providing a good/faulty system integrity result output responsive to operatively relating said first end second values;

means for activating said gaming system to said aiarm mode responsive to a result output of faulty system integrity; and

means for activating said gaming system to said player-responsive mode responsive to a result output of good system integrity.

49. The system as in Claim 48:

wherain said first relationship has the characteristic that changing the contents of said first memory changas said first value.

50. A gaming system as in Claim 48 or 49:

wherein said validation information is derived from said first value.

51. The system as in Claim 48 wherein said first, second and inverse second relationships are one-way functions.

52. A system for insuring the integrity of information loaded into the system, comprising:

(a) a memory having initially undefined contents;

(b) means for loading data and validation information into the contents of the memory wherein said data is related to said validation information according to a public first and a secret second relationship;

(c) means for verifying the integrity of the loaded contents comprising:

(1) means for deriving a first value according to the first relationship responsive to the data contents of the memory,

(2) means for deriving a second value according to a public inverse of the second relationship responsive to the validation information,

(3) means for operatively relating the first and second values to provide an integrity output indicative of good and bad integrity of the memory contents,

(d) means for controlling the operable status of the system further comprising:

(1) means for activating said system to a normal operational mode responsive to the good integrity output, and

(2) means for activating said system to an alarm mode responsive to said bad integrity output.

53. The system as in Claim 52:

wherein said system is a gaming system.

54. The system as in Claim 53 further comprising:

an interface port for communicating with an external device;

means responsive to said interface port for loading said memory with the communications received from said external device.

55. The system as in Claim 53 or 54 wherein said memory is located in a nonsecure portion of the second system, and said means for verifying the integrity and means for controlling the operable status are located in a secure portion of the second system.

56. The system as in Claim 52 or 53 having user responsive input means, wherein said normal operational mode is further characterized as being responsive to said user responsive input means.

57. A method of controlling the operable mode of a system having a memory with data and validation information contents, comprising the steps of:

deriving a first value from the data contents according to a first relationship,

deriving a second value from the validation information according to a second relationship;

operatively relating said first and second values so as to determine system integrity,

activating the system to a selected operative mode responsive to the determined system integrity.

58. The method as in Claim 57 further characterized in that said system is a gaming system.

59. The method as in Claim 57 further characterized in that said validation information is derived from said data content according to the first relationship and an inverse to the second relationship.

60. The method as in Claim 59 further comprising the steps of:

activating the system to a normal operative mode responsive to a determination of good system integrity, and

activating said system to an alarm operative mode responsive to a determination of bad system integrity.

61. The method as in Claim 57 or 58 further comprising the steps of:

making the first and second relationships public;

maintaining the inverse to the second relationship in secrecy.

62. The method as in Claim 57 or 58 further comprising the steps of:

deriving said first value by means of a function which exhibits the characteristic that changing any of the contents of the nonsecure memory changes the first value.

63. The method as in Claim 62 wherein said validation information is derived from said first value, further comprising the steps of:

determining said second value from said validation information by means of an inverse derivation to that by which the validation information is obtained from the first value.

64. A method for creating a memory having verifiable secure data contents comprising the steps of:

deriving a first value from the data contents of the memory by a first relationship wherein changing the contents of the memory changes the first value;

deriving a validation value from said first value by a second relationship having an inverse relationship; and

storing and validation value in said memory contents.

65. A method of verifying the integrity of a memory having data content and validation value content related to said data content by first and second relationships, comprising the steps of:

deriving a first value from the data content of the memory by the first relationship;

deriving a second value from said validation value by an inverse to said second relationship;

providing an integrity output indicative of good and bad system integrity responsive to operatively relating the first value and the second value;

providing a first activation signal responsive to said integrity output indicating good system integrity and

providing e second ectivation signal responsive to said integrity output indicating bad system intagrity.

66. The method of Claim 64 or 65 wherein sald first relationship end inverse second reletionship ere public end said second raletionship is secret.

68. In e system, heving e seeled secure circuit portion comprising a processor and a first memory, seld system also heving en insecure circuit portion comprising e second memory, e method of insuring tha intagrity of the insecure portion of the system comprising the steps of:

deriving e first velue from the dete content of the second memory by e first reletionship wherein chenging the contents of the second memory changes the first value;

deriving e velidation value from seld first value by a second relationship having en inverse relationship end

storing sald velidetion velue et e predefined location in said second memory.

69. The method es in Cleim 68 further comprising the steps of:

(a) verifying the integrity of the second memory by means of seld secure portion, further comprising the steps of:

(1) deriving e third velue from the contents of the second memory by sald first reletionship;

(2) deriving e fourth velue from seid velidetion value by seid inverse relationship; end

(3) operetively releting the third velue to the fourth value and providing e relationel output; end

(b) controlling the operable stetus of the system further comprising the steps of:

(1) ectivating seid geming system to a normel-responsive mode responsive to said reietional output indicating good system integrity, end

(2) ectivating the system to en alarm mode responsive to said relationel output indicating bad system integrity.

70. The method of Claim 68 or 69 further cheracterized in thet seld first end inverse second relationships are public and said second reletionship is secret.

71. The method of Claim 70 further characterized in that said second memory is nonvoletile.

72. The method of Claim 68 or 69 further charactarized in that system is a geming system.

73. The method of Claim 69 further characterized in thet said normel-responsive mode is a player responsive mode, end said alerm mode is a player nonresponsive mode.

74. A method of Claim 71 wherein said step of operatively relating further comprises the steps of:

comparing the magnitude of said first and second veiues, end indicating seid good system integrity by a reletional result of equelity, and indicating sald bad system integrity by e reletional result of inequality.

75. The method of Claim 71 further cheracterized in thet seld first, second and inverse second reletionships ere one-wey mapping functions.

76. In e gaming system, having e player responsive mode end e pleyer nonresponsive elerm mode, aeid system comprising e nonsecure memory heving data end velidation information, seld velidetion information being operatively related to the date, said sytem also heving e secure memory, e method for selectively activating the system to a predetermined mode responsive to validating the integrity of the nonsecure memory, comprising the steps of:

(e) executing instructions from the secure memory so es to darive e first value representative of the contents of the nonsecure memory;

(b) executing instructions from the secure memory so as to derive e second value represantative of the velidetion word;

(c) operatively releting the first and second values to provide en indication of system integrity;

(d) ectivating seid gaming system to said player nonresponsive elerm mode responsive to en indication of improper system integrity;

(e) activating seid gaming system to seid player-responsive mode responsive to an indication of good system integrity.

77. The method as in Cleim 76 further comprising the steps of:

deriving sald first velue by means of a function which exhibits the characteristic that chenging any of the contents of the nonsecure memory chenges the first velue.

78. The method es in Cleim 77:

wherein said validation word is derived from said first value, further comprising the steps of:

determining said second value from said validation word by means of en inverse derivation to that by which the validation word is obtained from the first value.

79. The method es in Claim 76 wherein said first velue is derived by

operatively relating seld deta to a first functionel mepping; and

further characterized in thet said validetion information is operatively related to sald first value eccording to e second functionel mapping,

wherein said second value is derived by

operatively releting said velidetion information to an inverse of said second functional mapping

80. The method of Claim 57 or 58 or 76 further comprising the steps of:

communicating seid data and associeted validation information to the system from e source externel to the system;

storing said communicated deta and associated velidetion informetion in seid memory.

81. A method for controlling the operative mode of e system, having local and remote devices

responsive to determined integrity of communicated information comprising the steps of:

operating upon data information at the remote device according to first and second relationships to derive validation information,

communicating said data and validation information from the remote device to the local device,

operating upon said data information at the local device, according to said first relationship, to derive a first value;

operating upon said validation information at said local device, according to an inverse of said second relationship, to derive a second value;

controlling the operative mode of the system responsive to operatively relating said first and second values.

82. The method as in Claim 81 further characterized in that there are a plurality of local devices, wherein the step of controlling the operative mode of the system further comprises the steps of:

selectively controlling the operative mode of each of said local devices responsive to the operative relationships for each respective first and second values.

83. The method as in Claim 81 further comprising the steps of:

deriving said first value by means of a function which exhibits the characteristic that changing any of the contents of the nonsecure memory changes the first value.

84. The method as in Claim 81 wherein said validation information is derived from said first value, further comprising the steps of:

determining said second value from said validation information by means of an inverse derivation to that by which the validation word is obtained from the first value.

85. The method as in Claim 81 further characterized in that said first and inverse second functional relationships are public, and said second functional relationship is secret.

86. The method as in Claim 81 or 85 further characterized in that said first, second and inverse second functional relationships are one-way functions.

87. A system for selectively operating in one of a plurality of modes responsive to a determined system integrity substantially as herein described with reference to the accompanying drawings.

88. A system for insuring the integrity of a remotely located downloaded memory substantially as herein described with reference to the accompanying drawings.

89. A gaming system substantially as herein described with reference to the accompanying drawings.

90. A gaming system operable in a player responsive mode and an alarm mode substantially as herein described with reference to the accompanying drawings.

91. A system for insuring the integrity of information loaded into the system substantially as herein described with reference to the accompanying drawings.

92. A method of controlling the operable mode of a system having a memory with data and validation information contents substantially as herein described with reference to the accompanying drawings.

93. A method for creating a memory having verifiable secure data contents substantially as herein described with reference to the accompanying drawings.

94. A method for verifying the integrity of a memory having data content and validaton value content related to said data content by first and second relationships substantially as herein described with reference to the accompanying drawings.

95. In a system, having a sealed secure circuit portion comprising a processor and a first memory, said system also having an insecure circuit portion comprising a second memory, a method of insuring the integrity of the insecure portion of the system substantially as herein described with reference to the accompanying drawings.

96. In a gaming system, having a player responsive mode and a player nonresponsive alarm mode, said system comprising a nonsecure memory having data and validation information, said validation information being operatively related to the data, said system also having a secure memory, a method for selectively activating the system to a predetermined mode responsive to validating the integrity of the nonsecure memory, substantially as herein described with reference to the accompanying drawings.

97. A method for controlling the operative mode of a system, having local and remote devices responsive to determined integrity of communicated information substantially as herein described with reference to the accompanying drawings.

Printed for Her Majesty's Stationery Office, by Croydon Printing Company Limited, Croydon, Surrey, 1983.
Published by The Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.